Caracterización Clásica de los Grupos Finitos Resolubles

Inés García Calavia

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Mª. Paz Jiménez
22 de Noviembre de 2019

Sumary

One of the most important result of the finite group (1872), are the Sylow Theorems. Let G be a finite group, let p be a prime, and let $|G| = p^a m$ with $p \nmid m$. A subgroup U of G with $|U| = p^a$ is called Sylow p-subgroup of G. Let π be a set of primes, a subgroup H of a group G is called Hall π-subgroup if $|H|$ is a π-number y $|G:H|$ is π'-number.

This thesis has the goal of demonstrate a characterization of the finite solvable groups using the Hall subgroups. The characterization that is demonstrated, in the 4th chapter, is the following theorem:

A finite group G is solvable if and only if it possesses Hall π-subgroups for all sets π of primes.

We start with an introduction in which we tell about the main theorems context and I explain how the proofs have been made in general and some of them in particular. Also, the sources of the proofs are mentioned.

The second chapter is composed by a collection of definitions and theorems that we use as the basis for the development of the proofs of the following chapters. Some of these definitions and theorems have been studied in the degree as a part of the subject Theory of Galois, these are the only ones that are not followed by a demonstration. Among other definitions we can find some characteristic subgroups of a group such as the subgroup

$$O_p(G) =< N | N \trianglelefteq G,\ N \quad p\text{-group} >= \cap\{P | P \in Syl_p(G)\}$$

and the Fitting subgroup of a finite group G is defined as follows, $F(G) =< O_p(G) | p \text{ prime } >$.

If K and H are subsets of G, we set $[K,H] =< [k,g] | k \in K, h \in H >$ with $[g,h] = g^{-1}h^{-1}gh$. Let H be a subset of a group G, we define the groups $N_G(H)$ and $C_G(H)$.

Every definition and annotations are reviewed in the Appendix so they can be easily found.

We would like to point out some results of this chapter that we consider more important or difficult.

Using a map of G on itself, by conjunction, it is proved that if order of G is a p prime power (is a p-group), its center is not trivial. Another important property of p-groups is if H is a proper subgroup of G, then $H < N_G(H)$.

The Fratinni argument says that let G be a finite group with a normal subgroup, N, and $P \in Syl_p(N)$, then $G = N_G(P)N$

Let G be a finite group, N is a minimal normal subgroup of G, N is direct product by isomorphis simple groups, in particular if G is solvable then N is q-elementary abelian subgroup.

Also, If G is solvable and $F(G)$ is a p-group, then $C_G(F(G)) \leq F(G)$

Let P be .a non-cyclic elementary abelian p-group and let Q be a elementary abelian q-group $Q \neq 1$ and $P \leq N_G(Q)$. Then there exists an element x in P, $x \leq 1$, such that $C_Q(x) > 1$

To end the chapter, it appears the Schur-Zassenhaus theorem that has a direct application in the final proof of the thesis. This theorem is very important at theory of the finite groups and maintains that if $N \trianglelefteq G$ assume that $|N| = n$ and $|G/N| = m$ are relatively prime, then $H \leq G$ exist as $H \cap N = 1$ y $HN = G$ (H is complement in G of N). We have demonstrated this result by adding the condition of N being abelian, since an easier proof is obtained and, with this restriction, the result is enough for its implementation in this thesis.

The third chapter is fully dedicated to the proof of the Burside's $p^a q^b$ theorem, which say that let G be a group of order $p^a q^b$, where p and q are primes, then G is solvable.

In particular, we suppose that the theorem is false, and let G be a counterexample of minimal order. The structure of G is carefully analysed, and evantually a contradiction is reached. This theorem is usually demonstrated in a short and direct way using the of character and representation theory, which we have avoided.

Some of the statements, in which the proof is divided, show characteristics of the G structure or some of its subgroups unlike others that serve as basis to understand and develop further results, such as the definition of locally central subgroup. We can see that the minimal counterexample verifies that, fixing s and r the two prime divisors of $|G|$, if $S \in s$-Sylow(G) and $1 \neq Y \trianglelefteq R \in Syl_r(G)$, then $G =< S, Y >$. We will see later that the Fitting subgroup of a subgroup, M, maximal of G, $F(M)$, has prime power order and we will prove that G has odd order before ending with the contradiction that G has to be a solvable group.

In the fourth chapter we introduce the concept of Hall π-subgroup and some of its properties.

First of all, we prove that if G is solvable and let π be a set of prime, then, there exist H subgroups such as $|H| = \pi$-number and $|G : H| = \pi'$-number. For this part, the Schur-Zassenhaus theorem is essential.

For the other implication, we try a result a little bit stronger. For this, we need to know if the G group has three solvable groups H_1, H_2 and H_3 whose indices are compressed two by two, then G is also solvable. And with this result and the Burside theorem of the 3rd chapter, we demonstrate the following:

Let G be a group, let $|G| = \prod_{j=1}^{r} p_i^{a_i}$, where $p_1, \cdots, p_r$ are distinct primes. Assume that G possesses subgroups $S_i \leq G$ such that $|G : S_i| = p_i^{a_i}$, then G is solvable.

A G group that has Hall π-subgroups for the whole π prime set, has this type of S_i subgroups and, therefore, G would be solvable. This way is how we get the characterization.

Índice general

Capítulo 1

Introducción

En este trabajo nos centramos en la teoría clásica de grupos finitos abstractos para dar una importante caracterización de los grupos resolubles. El concepto de grupo que introdujo Galois, como conjunto de ciertas permutaciones de las raíces de un polinomio, sirvió para caracterizar el hecho de que estas raíces pudieran ser una expresión de radicales a partir de los coeficientes del propio polinomio.

Galois consiguió asociar a cada polinomio un grupo de permutaciones unívocamente determinado, su grupo de Galois. A partir de la estructura de estos grupos se determinará si el polinomio es resoluble por radicales. Concretamente, sus raíces se pueden representar con expresiones de radicales a partir de sus coeficientes si y solo si su grupo de Galois asociado es resoluble. Para ello, definió el concepto de grupo resoluble como extensiones de grupos abelianos, esta es:

Un grupo G se dice resoluble si existen subgrupos G_i verificando:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

tal que G_{i+1}/G_i con $i = 0, 1, \cdots, k-1$ son abelianos.

El objetivo de este trabajo es llegar a probar el siguiente resultado que caracteriza los grupos finitos resolubles:

Un grupo finito G es resoluble si y solo si posee π-subgrupos de Hall para todo conjunto de primos π.

Las demostraciones son completas y autocontenidas, es decir, todo lo que hemos utilizado para su desarrollo se encuentra en el mismo trabajo, en el cual lo único que daremos por demostrado serán aquellos resultados que aparecen en la asignatura de Teoría de Galois. En general, aunque no hay ninguna demostración original, si que hemos ido buscando el camino en distintos libros para basarnos sólo en la estructura del grupo e introducir el menor número de conceptos posibles.

Uno de los pilares de la demostración es el conocido como Teorema paqb de Burside, el cual dice que si $|G| = p^a q^b$ siendo p y q primos distintos, entonces G es resoluble. La demostración original de Burside, publicada en 1904, es corta y elegante pero necesita de la teoría de representaciones y caracteres tal como se suele encontrar comúnmente en los libros de Teoría de Grupos, por ejemplo, en el libro *An Introduction to Ideas and Methods of the Theory of Groups* [2]. Pero, puesto que no se han estudiado estas teorías en el grado, damos una demostración directa adentrándonos en la estructura de un grupo con unas determinadas condiciones, siguiendo el capítulo de *Introducción a los grupos resolubles* del libro [1]. Aquí seguimos la linea de esta demostración, aunque allí no es autocontenida.

También es imprescindible el teorema de Schur-Zassenhaus cuyo enunciado dice:

Si $N \leq G$ tal que $|N|$ y $|G/N|$ son primos entre sí, existe $H \leq G$ cumpliendo $NH = G \quad N \cap H = 1$

En la mayoría de los libros su demostración aparece como aplicación de la teoría de cohomología de grupos, que también se ha evitado en este trabajo. La demostración que ponemos aquí, la hemos extraido de [6], pero le hemos añadido una restricción, ya que damos la demostración solo para el caso en el que la necesitamos. Concretamente introducimos a la hipótesis del teorema que N es abeliano, esto hace que la demostración sea más sencilla.

En otros muchos casos hemos simplificado las demostraciones cambiando el resultado para adaptarlo a los casos en los que lo necesitamos, normalmente más particulares que el caso general.

Muchos de los resultados que aparecen son pues lo contrario de generalizaciones, son adaptaciones necesarias para llegar al objetivo del trabajo.

Capítulo 2

Definiciones y teoremas previos.

Definición 2.1. Un grupo es un conjunto no vacío G dotado de una operación binaria interna, que denotamos $\cdot$, y que verifica:

1. Es asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall$ a,b,c $\in G$.
2. Existe elemento neutro, $1 \in G$ tal que $1 \cdot g = g = g \cdot 1$ $\forall g \in G$.
3. Existe elemento inverso $x^{-1} \in G \forall x \in G$ tal que $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Si G es finito, llamamos orden de G su número de elementos. Este número se denota $|G|$.
En todo el trabajo G será, salvo que se diga otra cosa, un grupo finito.

Definición 2.2. Un subgrupo de un grupo G es un subconjunto de G con la operación restringida y que verifica los axiomas de la definición de grupo.
Si H es subgrupo de G, escribimos $H \leq G$.

Definición 2.3. Dados dos subgrupos A y B de G, denotamos al conjunto $AB = \{ab | a \in A \text{ y } b \in B\}$.

Lema 2.4. *Sean U, V y W subgrupos de G con $V \leq U$, entonces $U \cap VW = V(U \cap W)$*

Demostración. Sea $vp \in V(U \cap W)$ con $v \in V, p \in (U \cap W)$, obviamente $vp \in VU = U$ y $vp \in VW$. Luego tenemos el contenido

$$V(U \cap W) \subseteq U \cap VW.$$

Sea $u = vw \in U \cap VW$,con $u \in U, v \in V$ y $w \in W$, entonces $v^{-1}u = w \in VU \cap W = U \cap W$. Por lo tanto $u \in V(U \cap W)$ y por doble contenido tenemos que

$$V(U \cap W) = U \cap VW.$$

□

Definición 2.5. Sea $H \leq G$ y $x \in G$, entonces:
$Hx = \{hx | h \in H\}$ se llama coclase a derecha módulo H y
$xH = \{xh | h \in H\}$ se llama coclase a izquierda módulo H.

En general $Hx \neq xH$.

Se tiene que $|Hx| = |H|$ y las coclases a derecha (a izquierda) forman una partición de G.

Definición 2.6. Si $H \leq G$, llamaremos índice de H en G al número de coclases a derecha (o a izquierda) y lo denotamos $|G : H|$.

Teorema 2.7. *1. (Lagrange) Si $H \leq G$, se tiene*

$$|G| = |G : H||H|.$$

2. Si $H \leq K \leq G$ se tiene

$$|G:H| = |G:K||K:H|.$$

Proposición 2.8. *Sean U y V subgrupos de un grupo G. Entonces:*

$$|UV||U \cap V| = |U||V|.$$

Y si $UV \leq G$

$$|UV:V| = |U:U \cap V|.$$

Definición 2.9. Un homomorfismo entre dos grupos $(G,\cdot)$ y $(H,\cdot)$ es una aplicación $f: G \to H$ tal que $f(a \cdot b) = f(a) \cdot f(b)$ para todo a, b $\in G$.

Si un homomorfismo es biyectivo se llamará isomorfismo.

Teoremas de isomorfía

Teorema 2.10. *a)* 1^{er} *Teorema de Isomorfía.*

Sea $f: G \longrightarrow H$ un homomorfismo de grupos. La aplicación

$$\bar{f}: G/Kerf \longrightarrow f(G)$$

dada por $\bar{f}(xKerf) = f(x)$, es un isomorfismo de grupos.

$$\frac{G}{Kerf} \simeq f(G).$$

b) 2^{do} *Teorema de Isomorfía.*

Sea $N \trianglelefteq G$ y $H \leq G$, entonces $H \cap N \trianglelefteq H$ y

$$\frac{H}{H \cap N} \simeq \frac{NH}{N}.$$

c) 3^{ro}*Teorema de Isomorfía*

Sea $N \trianglelefteq G$ y $M \trianglelefteq G$ con $N \subseteq M$, entonces

$$\frac{G}{M} \simeq \frac{G/N}{M/N}.$$

Proposición 2.11. *Sean U, V y W subgrupos de un grupo finito G. Si m.c.d.$(|G:U|, |G:V|) = 1$,o simplemente $(|G:U|, |G:V|) = 1$, entonces $G = UV$ y $|G:(U \cap V)| = |G:U||G:V|$.*

Demostración. Sea $D = U \cap V$ por el teorema de Lagrange los números coprimos $|G:U|$ y $|G:V|$, ambos, dividen a $|G:D|$, y por lo tanto $|G:D| = m|G:U||G:V|$ para algún natural m. Aplicamos el teorema de Lagrange a ambos lados de la igualdad

$$\frac{|G|}{|D|} = |G:D| = m|G:U||G:V| = m\frac{|G|}{|U|}\frac{|G|}{|V|}$$

$$\frac{|U||V|}{|D|} = m|G|.$$

Y por (2,8) tenemos

$$m|G| = \frac{|U||V|}{|D|} = |UV| \leq |G|.$$

Luego tiene que ser $m = 1$, $G = UV$ y $|G:D| = |G:U||G:V|$. □

Definición 2.12. Sea G un grupo y $g \in G$, denotamos $x^g = g^{-1}xg$ al conjugado de x por g.

Definición 2.13. Un automorfismo es un isomorfismo de un grupo G sobre si mismo. Al conjunto de todos los automorfismos de un grupo se denota como $Aut(G)$.

La aplicación $\alpha_g : G \longrightarrow G$ definida por $\alpha_g(x) = x^g$, es un automorfismo de G denominado automorfismo interno de G. Al conjunto de todos los automorfismos internos de G se denota como $Int(G)$.

$Int(G)$ es un subgrupo normal de $Aut(G)$.

Definición 2.14. Un subgrupo H de G se dice que es normal y se escribe $H \trianglelefteq G$ cuando se verifica:

$$Hx = xH \quad \forall x \in G$$

equivalentemente

$$x^{-1}Hx = H \quad \forall x \in G$$

Esto no tiene porque significar que $xh_1 = h_1x$, si no que existen dos elemento de H, h_1 y h_2, tal que que se verifica que $xh_1 = h_2x$ teniendo en cuenta que estos dos elementos pueden ser iguales o distintos. Cuando esto sucede se dice que h_1 y h_2 son elementos conjugados.

Definición 2.15. La aplicación $G \longrightarrow G$ dada por $x \longrightarrow x^g = g^{-1}xg$ es un automorfismo de G. Sea H un subgrupo de G, entonces

$$H^g = g^{-1}Hg = \{g^{-1}hg | h \in H\}$$

también es un subgrupo de G llamado conjugado de H por g. Se tiene que H es isomorfo a H^g.

Definición 2.16. Usamos H^G para denotar al grupo

$$H^G = < H^g | g \in G >$$

de las conjugaciones de H en G.

Veamos que es el menor subgrupo normal de G que contiene a H.
Sea y un elemento de G, entonces $H^g = H^{gy^{-1}y}$. Como $H^{gy^{-1}} \leq H^G \Longrightarrow H^g \leq (H^G)^y$

Luego $H^G \leq (H^G)^y$ para cualquier y de G.

Definición 2.17. Sean G_1 y G_2 grupos. $G_1 \mathrm{x} G_2$ con la operación $(x_1,x_2)(y_1,y_2) = (x_1y_1, x_2y_2)$ para cada $x_1, y_1 \in G_1, \quad x_2, y_2 \in G_2$ es un grupo que se llama producto directo de G_1 y G_2.

Definición 2.18. Sea $\phi : H \longrightarrow Aut(N)$ un homomorfismo de grupos. En el conjunto de pares ordenados definimos la operación $(n_1,h_1)(n_2,h_2) = (n_1 n_2^{\phi(h_1^{-1})}, h_1h_2)$. Se tiene que es un grupo que se llama producto semidirecto de H por N via ϕ.

Definición 2.19. Sean U y V subgrupos de G, si $UV = G$ diremos que U y V son suplementarios en G y si además $V \cap U = 1$ entonces los llamaremos complementarios en G.

Lema 2.20. *Sea G un grupo:*

1. *Si $N, H \leq G$, $NH \leq G$ si y solo si $NH = HN$.*
2. *Si $N \trianglelefteq G$ y $H \leq G$, entonces $NH \leq G$.*
3. *Si $N \trianglelefteq G$ y $H \trianglelefteq G$, entonces $N \cap H \trianglelefteq G$ y $NH \trianglelefteq G$.*
4. *Si $N \trianglelefteq G$, $H \leq G$ y $N \cap H = 1$, entonces $NH = G$. Se dirá que G es producto semidirecto de N y H y se escribe $G = [N]H$.*

5. *Si $N \trianglelefteq G$, $H \trianglelefteq G$ y $N \cap H = 1$, entonces N y H conmutan. Se dirá que G es producto directo de N y H. Por lo tanto $G \simeq NxH$* (2,17).

6. *Si G es producto directo de N y H y $M \trianglelefteq N$, entonces $M \trianglelefteq G$.*

Definición 2.21. Sea $x \in G$, definimos $< x >= \{x^n | n \in \mathbb{Z}\}$, entendiendo $x^0 = 1$ y si $n > 0$, $x^n = x \cdots x$ (n veces)y si $n < 0$ $x^n = (x^{-n})^{-1} = x^{-1} \cdots x^{-1}$ (-n veces). Es decir que $< x >$ es el menor subgrupo de G que contiene a x. Si existe $x \in G$ tal que, $G =< x >$, se dice que G es cíclico.

Todos los subgrupos de un grupo cíclico también serán cíclicos.

Definición 2.22. Sea $x \in G$. Si existe un natural n tal que $x^n = 1$, al menor tal n se le llama orden de x. Si no existe este n se dice que x no tiene orden finito.

Notar que si x tiene orden n, se tiene que $x^{-1} = x^{n-1}$,así que todas las potencias de exponente negativo son potencias también de exponente positivo y

$$< x >= \{1, x, \cdots, x^{n-1}\}.$$

Definición 2.23. Sea C un conjunto tal que $C \subseteq G$, se denota por $< C >$ al subgrupo generado por C; Así

$$< C >= \cap\{U | C \subseteq U \leq G\}.$$

Definición 2.24. Un grupo o un subgrupo será denominado p-grupo o p-subgrupo, respectivamente, si su orden es potencia de p, con p primo.

Definición 2.25. Sea π un conjunto de números primos, se dice que un grupo G es π-grupo si todos los números primos divisores del orden de G pertenecen al conjunto π. Por el contrario, se dirá que G es un π'-grupo si ninguno de los primos que dividen al su orden pertenece al conjunto π.

De igual forma, un número entero será π-número si todos sus divisores primos están en el conjunto π, y será π'-número si ninguno de sus divisores primos está en π.

Lema 2.26. *Sea G un grupo cíclico cuyo orden es potencia de un primo, entonces el conjunto de los automorfismos de G también es cíclico.*

Definición 2.27. Un grupo se dirá abeliano si su operación binaria interna es conmutativa.

Un grupo elemental abeliano es un grupo abeliano en el cual todos los elementos no triviales tienen el mismo orden finito. De hecho es fácil ver que los elementos no triviales deben ser de orden primo, así cada grupo elemental abeliano es un p-grupo para algún p primo.

Definición 2.28. Sea G un grupo:

1. Para $g, h \in G$ tenemos el elemento $[g,h] = g^{-1}h^{-1}gh$ y lo llamaremos conmutador de g con h.

2. Si A y B son subconjuntos de G, se define el grupo

$$[A,B] =< [a,b] | a \in A, \quad b \in B > .$$

Definición 2.29. Un grupo se dice simple si no tiene subgrupos normales propios, es decir: G es simple si $N \trianglelefteq G \Longrightarrow N = 1$ ó $N = G$.

Un grupo abeliano es simple $\Longleftrightarrow$ es cíclico de orden primo.

Proposición 2.30. *Si $N \leq G$, el símbolo G/N denotará el conjunto de coclases a derecha de N en G. Cuando se cumple $N \trianglelefteq G$, el conjunto $G/N = \{Nx | x \in G\}$ es grupo con la operación $(Nx)(Ny) = Nxy$, al que denominamos grupo cociente.*

Definición 2.31. Una acción de un grupo G sobre un conjunto $C \neq \emptyset$ es un homomorfismo entre G y el grupo de las permutaciones de C.

$$\varphi : G \to Per_C.$$

Si no hay lugar a error, estará definida como $\varphi(g) : i \longrightarrow i^g$ o $\varphi(g)(i) = i^g$ para cada $i \in C$ y $g \in G$.

Si esta aplicación es inyectiva diremos que la acción es fiel o que G actúa fielmente sobre Per_C. A veces al conjunto de las permutaciones se le denota como S_C.

Definición 2.32. Subgrupo característico

Un subgrupo H de un grupo G es llamado característico si para cualquier $\phi \in Aut(G)$ se cumple que $\phi(H) = H$. En otras palabras, significa que cada automorfismo de G transforma a H en si mismo.

A estos subgrupos se les denota por, $HcharG$.

Proposición 2.33. *Sea G un grupo:*

1. *Si H char G, entonces H es subgrupo normal de G.*

   Demostración. Para un $g \in G$ la conjugación $\phi_g : G \longrightarrow G$ definida por $\phi_g(x) = x^g$, que es un automorfismo de G.

   Como H es subgrupo característico de G, $\phi_g(H) = H^g = H \quad \forall g \in G$ por lo tanto H es subgrupo normal de G. □

2. *Si H es el único subgrupo de G de un orden determinado, entonces H char G.*

   Demostración. Para cualquier automorfismo $\phi \in Aut(G)$, tenemos $\phi(H) \subset \phi(G) = G$ y $|H| = |\phi(H)|$. La unicidad de H implica que $H = \phi(H)$ y por lo tanto H es característico. □

3. *Supongamos que un subgrupo K es característico de un grupo H, y que este grupo H es normal en G, entonces K también es normal en G.*

   Demostración. Tomamos $g \in G$ y consideramos el automorfismo conjugación ϕ_g de G, conjugar por g. Como $H \trianglelefteq G$, tenemos que $\phi_g(H) = H$, por lo tanto la restricción $\phi_{g|H}$ pertenece a $Aut(H.)$ Ahora como K es característico in H, tenemos que $\phi_{g|H}(K) = K$, o equivalentemente que $g^{-1}Kg = K$, luego K es normal en G. □

Definición 2.34. Sea p un primo y G un p-grupo. Definimos el subgrupo característico $\Omega(G)$ de la siguiente forma:

$$\Omega(G) =< g \in G | g^p = 1 > .$$

Definición 2.35. Sea el conjunto finito $C \neq \emptyset$ y G grupo actuando sobre C. Sea $i \in G$:

a) La órbita de i es $\{i^g | g \in G\}$ y se denota $\theta(i)$.

b) El estabilizador de i es $St(i) = \{g \in G | i^g = i\}$. Se tendrá que $St(i) \leqslant G$.

Y se tiene que $|\theta(i)| = \dfrac{|G|}{|St(i)|}$.

Definición 2.36. Una acción, φ, de un grupo G sobre un conjunto C se dice transitiva, o que G actúa transitivamente sobre un conjunto C, si para todo par cualesquiera i y j del conjunto C existe un $g \in G$ tal que $\varphi(g)(i) = j$.

Definición 2.37. Consideramos la acción de un grupo G sobre si mismo, dada por la aplicación

$$\varphi : G \longrightarrow Per_G$$

definida como $\varphi(g) : x \longrightarrow x^g$ para cada $x \in G$.

El centro de un grupo G es el núcleo de esta acción, se escribe

$$Z(G) = \{g \in G | x^g = x \quad \forall x \in G\} = \{g \in G | xg = gx \quad \forall x \in G\}.$$

A las órbitas de esta acción se les llama clase de conjugación de G,

$$Cl_G(x) = \{x^g | g \in G\}.$$

Y al estabilizador de un elemento $x \in G$ se le llama centralizador de x en G

$$C_G(x) = \{g \in G | xg = gx\}.$$

El centralizador de un subgrupo es : $C_G(H) = \{g \in G | hx = xh \quad \forall h \in H\}$.

Definición 2.38. El normalizador de H en G es el subgrupo:

$$N_G(H) = \{g \in G | g^{-1}Hg = H\}.$$

El normalizador es el subgrupo más grande en el que M es normal y se tendrá que

$$C_G(H) \leq N_G(H).$$

Observación: Sean $H \leq G$ y el conjunto de todos los subgrupos de G conjugados con H

$$\{H^g | g \in G\} = \mathscr{S}.$$

La aplicación

$$\varphi : G \longrightarrow Per_{\mathscr{S}}$$

dada por $\varphi(x) : H^g \longrightarrow H^{gx}$ es una acción transitiva de G sobre $\mathscr{S}$.

$\forall \quad gx \in G, H^{gx} \in \mathscr{S}$ la acción está bien definida. Y para probar que es transitiva bastaría con tomar $x = g_1^{-1}g_2$ y $H^{g_1} \in \mathscr{S}$ que bajo la acción anterior $\varphi(g_1^{-1}g_2)(H^{g_1}) = H^{g_1 g_1^{-1} g_2} = H^{g_2} \in \mathscr{S}$.

Por lo tanto se tendrá que

$$|\mathscr{S}| = \frac{|G|}{|N_G(H)|}.$$

En particular, el número de conjugaciones con H divide al orden de G y $|G : N_G(H)|$ también es divisor de $|G|$.

Definición 2.39. Un grupo G se dice resoluble si existen subgrupos G_i verificando:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$$

tal que G_{i+1}/G_i con $i = 0, 1, \cdots, k-1$ son abelianos.

Es decir, un grupo será resoluble cuando exista una cadena de eslabones abelianos.

Un grupo simple resoluble es cíclico de orden primo.

Teorema 2.40. *Si $N \trianglelefteq G$ entonces N y G/N son resolubles si y solo si G es resoluble.*

Lema 2.41. *Sea G tal que $|G| = p^n$ con p primo y $N \trianglelefteq G$, entonces $N \cap Z(G) \neq 1$ y en particular $Z(G) \neq \{1\}$.*

Demostración. Sea la acción $\phi : G \longrightarrow Per_N$ dada por $\phi(g) : x \longrightarrow x^g \quad \forall x \in N$.

Sean $\theta(x_1), \theta(x_2), \cdots, \theta(x_r)$ las distintas órbitas. Como el conjunto de las órbitas forman una partición.

$$|N| = |\theta(x_1)| + |\theta(x_2)| + \cdots + |\theta(x_r)|. \tag{2.1}$$

Además:

$$|\theta(x_i)| = |G|/|C_G(x_i)| = 1 \quad o \quad \text{potencia de } p$$

será 1 si y solo si el elemento cuya órbita estamos mirando pertenece al centro del grupo, G, por el contrario, si no pertenece, sabemos que el estabilizador es un subgrupo de G y por lo tanto su orden es divisor del orden de G, luego $|C_G(x_i)| = p^k$ para algún $k < n$.

Si $N \cap Z(G) = 1$ solo la órbita de este elemento tendrá orden 1, el resto de órbitas serán de orden potencia de p o, equivalentemente, serán múltiplos de p. Se tendrá que 2,1 $p^{n'} = 1 + mp$. Esto no es posible ya que $1 + mp$ no es múltiplo de p y $p^{n'}$ sí.

Por lo tanto concluimos que $N \cap Z(G) \neq 1$ y en particular $Z(G) \neq \{1\}$. □

Proposición 2.42. *Sea un grupo G tal que $|G| = p^n$ con p primo y H subgrupo propio de G entonces, H está contenido estrictamente en el normalizador, $H < N_G(H)$.*

Demostración. Si H es subgrupo normal de G no habría nada que demostrar pues, $g^{-1}Hg = H \quad \forall g \in G \Longrightarrow N_G(H) = G \neq H$.

Entonces asumimos que H no es normal en G y sea $\mathsf{S} = \{H^a, H^b, \cdots\}$ el conjunto de los conjugados de H distintos de H. Sabemos que $|G : N_G(H)|$ divide al orden de G, por lo tanto, será potencia de p. Entonces $|\mathsf{S}| = |G : N_G(H)| - 1 = p^k - 1$ para algún k, esto se sigue de la observación anterior.

Sea la acción $\varphi : H \longrightarrow Per_{\mathsf{S}}$ dada por $\varphi(h) : H^g \longrightarrow (H^g)^h$, que está bien definida pues si cunjugamos los elementos de S con uno de H el resultado sigue perteneciendo a S. Como $|\mathsf{S}| = p^k - 1$ al menos una de las órbitas de esta acción tendrá orden 1, luego esta órbita tendrá un único elemento. Sea $H^g \in \mathsf{S}$ dicho elemento tal que $(H^g)^a = H^g \forall a \in H$, entonces

$$(ga)^{-1}H(ga) = g^{-1}Hg$$

$$(gag^{-1})^{-1}H(gag^{-1}) = H$$

$$\Longrightarrow (gag^{-1}) \in N_G(H) \quad \forall a \in H \Longrightarrow H^{g^{-1}} \subseteq N_G(H)$$

Como $H \neq H^{g^{-1}} \leq N_G(H)$ se tendrá que

$$H < N_G(H).$$

□

Proposición 2.43. *Sea G un grupo finito y N un subgrupo normal minimal de G. Se tiene que N es un producto directo de subgrupos $S_1, \cdots, S_k$ tales que son simples e isomorfos entre sí. En particular si G es abeliano N es p-elemental abeliano para algún primo p.*

Demostración. Los subgrupos característicos en N son normales en G, luego por la minimalidad de N, se tiene que no tiene subgrupos característicos propios (N es característicamente simple). Si N no es simple sea $S = S_1$ un subgrupo normal minimal de N. Existe $\alpha \in Aut(N)$ tal que $S^\alpha \neq S$ y se tendría que es otro subgrupo normal minimal de N luego $S^\alpha \cap S = 1$ y $S^\alpha S$ es un producto directo que escribimos $S^\alpha \times S$, sea M el mayor subgrupo de N que sea producto directo de algunos S^α siendo $\alpha \in Aut(N)$.

Si existiera $\alpha \in Aut(N)$ tal que $S^\alpha \not\leq M$ se tendría $M \cap S^\alpha = 1$ por la minimalidad de S^α y MS^α sería un producto directo en contra de ser M el máximo. Se tiene pues que para todo $\alpha \in Aut(N)$, $M^\alpha = M$ característico en N, luego $M = N$.

Tenemos pues que $N = S_1 \times \cdots \times S_k$ tales que $S_i \simeq S$ para todo i. Observamos que los subgrupos normales de $S_1 = S$ son subgrupos normales de N y por la minimalidad de S, se tiene que debe ser simple.

Si G es resoluble, también lo son N y S, luego S es cíclico de orden p para algún primo p. □

Teoremas de Sylow

Teorema 2.44. *Sea un grupo finito G, para cada primo p divisor del orden de G existen subgrupos de orden la máxima potencia de p que divide al orden de G. Estos subgrupos se llamarán p-subgrupos de Sylow de G o p-Sylow de G. Denotaremos al conjunto de los p-subgrupos de Sylow de G* $Syl_p(G)$.

Teorema 2.45. *Sea G un grupo finito y p un primo divisor del orden de G. Si H es un subgrupo de G de orden potencia de p y P es un p-subgrupo de Sylow de G, entonces existe* $g \in G$ *tal que* $H \leq P^g$.

Corolario 2.46. *Si P y Q son p-subgrupos de Sylow de G, existirá* $g \in G$ *tal que* $Q = P^g$.

Lema 2.47. *Sea G un grupo finito y p un primo divisor de* $|G|$.

Sea $\{p_1, p_2\}$*el conjunto completo de los primos divisores de* $|G|$ *y sea* $P_i \in Syl_{p_i}(G)$ *con* $i = 1,2$, *entonces* $G =< P_1, P_2 >= P_1P_2$.

Demostración. b. Tenemos que

$$|P_1P_2| = \frac{|P_1||P_2|}{P_1 \cap P_2} = |G|$$

siendo $P_1 \cap P_2 = 1$ porque P_1 y P_2 son subgrupos de Sylow cuyos ordenes son primos entre si. □

Definición 2.48. Un grupo G se dice nilpotente si es producto directo de sus subgrupos de Sylow.

Todo grupo nilpotente es resoluble.

Definición 2.49. Sea π un conjunto de números primos y G un grupo finito.

a) Para un p primo definimos el conjunto

$$O_p(G) = \cap\{P | P \in Syl_p(G)\}.$$

Se tiene que $O_p(G)$ es el mayor p-subgrupo normal de G.

b) El subgrupo $O_\pi(G)$ de G está definido como:

$$O_\pi(G) =< N | N \trianglelefteq G, N \text{ un } \pi\text{-grupo} > .$$

Más adelante tomaremos $\pi = p'$ que denotará al conjunto de todos los primos divisores del orden de G distintos a p.

Definición 2.50. El subgrupo Fitting, F(G), de un grupo finito G es definido como:

$$F(G) =< O_p(G) | p \text{ primo} >$$

siendo $\sigma(G)$ los primos divisores del orden de G. Es claro para esta definición que $F(G)$ es producto directo

$$F(G) = O_{p_1}(G)x \cdots xO_{p_n}(G)$$

para los p_i primos divisores de $|G|$ y que $O_p(G) \in Syl_p(F(G))$.

Lema 2.51. ***El argumento de Frattini***

Si G es un grupo finito con un subgrupo normal H y P es un p-Sylow de H, entonces $G = N_G(P)H$.

Demostración. Por los teoremas de Sylow sabemos que todo p-subgrupo de Sylow de H es H-conjugado de P, es decir, serán de la forma $h^{-1}Ph$ para algún $h \in H$.

Sea $g \in G$, como H es normal en G el subgrupo $g^{-1}Pg \subseteq H$, luego será un p-subgrupo de Sylow de H. Por lo anterior, este p-subgrupo de Sylow debe ser H-conjugado de P para algún $h \in H$, entonces

$$g^{-1}Pg = h^{-1}Ph \Longrightarrow hg^{-1}Pgh^{-1} = P.$$

De donde se sigue que $(gh^{-1}) \in N_G(P)$ y por tanto $g \in N_G(P)H$.

Tenemos el contenido

$$G \subseteq N_G(P)H = HN_G(P)$$

y como el otro contenido es trivial queda demostrado que

$$G = N_G(P)H.$$

□

Lema 2.52. *Sea P un p-subgrupo de G, N un p'-subgrupo normal de G, entonces:*

$$N_G(P)N/N = N_{G/N}(PN/N).$$

Demostración. Procedemos por doble contenido. Es claro que $\frac{N_G(P)N}{N} \leq N_{G/N}(\frac{PN}{N}) = \frac{U}{N}$; veamos ahora el otro contenido.

Como $U/N = N_{G/N}(PN/N)$, entonces $PN \trianglelefteq U$ y $P \in Syl_p(PN)$. Por los Teoremas de Sylow y el argumento de Frattini tendremos que:

$$U = N_U(P)PN = N_U(P)N.$$

Pero $N_G(P)N \leq U$, y por lo tanto $U = N_G(P)N$. □

Proposición 2.53. *Sea G grupo finito resoluble y tal que $F(G)$ es un p-grupo, entonces*

$$C_G(F(G)) \leq F(G)$$

.

Demostración. También es cierto cuando $F(G)$ no es un p-grupo pero a lo largo del trabajo solo necesitamos el caso que vamos a demostrar.

Procedemos por reducción a lo absurdo; supongamos que $C_G(F(G)) > F(G)$ luego existe un subgrupo normal minimal no trivial $N/F(G)$ q-elemental abeliano para algún q primo de $\frac{C_G(F(G))F(G)}{F(G)}$. Sea $M = N \cap C_G(F(G)) \trianglelefteq G$, se tiene que:

$$\frac{N \cap C_G(F(G))}{F(G) \cap C_G(F(G))} = \frac{N \cap C_G(F(G))}{F(G) \cap N \cap C_G(F(G))} \simeq \frac{F(G)(N \cap C_G(F(G)))}{F(G)} = \frac{N \cap C_G(F(G))F(G)}{F(G)} = \frac{N}{F(G)}$$

q-elemental abeliano.

Como $F(G) \cap C_G(F(G)) = Z(F(G))$ es un p- grupo se pueden dar dos casos; que $q = p$, en cuyo caso M es un p-grupo normal en G y por tanto $M \leq F(G)$ o que sean primos distintos, así $F(G) \cap C_G(F(G)) = Z(F(G))$ será un p-subgrupo de Sylow de M y, obviamente, normal en M.

Los elementos de M conmutan con todos los de $F(G)$, si consideramos Q un q-subgrupo de Sylow de M, se tiene que $M = QZ(F(G))$ y Q conmuta con todos los elementos de $F(G)$, luego Q es normal en M. Así M es nilpotente y por tanto

$$M = N \cap C_G(F(G)) \leq F(G).$$

En los dos casos hemos llegado a que $M \leq F(G)$, luego

$$N \cap C_G(F(G)) = F(G) \cap C_G(F(G)) \Longrightarrow N/F(G) = 1,$$

por lo que $N = F(G)$, $C_G(F(G))F(G) = F(G)$ y $\quad C_G(F(G)) \leq F(G)$. □

Lema 2.54. *Sea G un grupo resoluble y P un p-subgrupo de G, entonces $O_{p'}(C_G(P))$ y $O_{p'}(N_G(P))$ están contenidos en $O_{p'}(G)$.*

Demostración. Sabemos que $C_G(P) \trianglelefteq N_G(P)$ y como todo $M \in O_{p'}(C_G(P))$ es un p'-grupo y cumple $M \trianglelefteq C_G(P)$, tenemos que $O_{p'}(C_G(P)) \leq O_{p'}(N_G(P))$. Por lo tanto solo tenemos que probar que $O_{p'}(N_G(P)) \leq O_{p'}(G)$ que lo haremos por inducción sobre $|G|$.

Para simplificar la notación en esta demostración denotaremos:

$$N_G(P) \approx N; \quad C_G(P) \approx C; \quad O_{p'}(G) \approx K$$

Primero supongamos que $K \neq 1$, la inducción produce que $O_{p'}(N_{G/K}(PK/K)) \leq O_{p'}(G/K) = 1$. Como P es un p-subgrupo de G y K es p'-subgrupo normal de G aplicando 2,52 tenemos que $N_{G/K}(PK/K) = NK/K$, obtendremos que

$$O_{p'}(N)K/K \leq O_{p'}(NK/K) = O_{p'}(N_{g/k}(PK/K)) \leq O_{p'}(G/K) = 1$$

Y por lo tanto $O_{p'}(N) \leq K$.

Ahora supongamos que $K = 1$ y por lo tanto $O_p(G) = F(G)$. Observamos que $O_p(G) \trianglelefteq N$ y $O_{p'}(N) \trianglelefteq N$, y además $O_p(G) \cap O_{p'}(G) = 1$ en consecuencia se tiene que estos dos subgrupos conmutan y tendremos

$$O_{p'}(N) \leq C_G(O_p(G)) = C_G(F(G)) \underbrace{\leq}_{2,53} F(G) \text{ que es p-grupo.}$$

Por lo que concluimos que $O_{p'}(N) = 1 = O_{p'}(G)$ y el lema queda demostrado. □

Proposición 2.55. *Sean P y Q subgrupos de G respectivamente p- elemental abeliano no cíclico y q-elemental abeliano y tales que $P \leq N_G(Q)$. Se tiene que existe $1 \neq x \in P$ tal que $1 < C_Q(x)$.*

Demostración. Como P tiene un subgrupo p elemental abeliano de orden p^2, podemos considerar que P es p- elemental abeliano de orden p^2.

Por reducción al absurdo supongamos que para todo $1 \neq x \in P$, si $y \in Q$ y $y^x = y$, entonces se tiene que $y = 1$.

Sea $1 \neq y \in Q$ y sean $g_1 = 1, g_2, \cdots g_n$ todos los elementos de P ($n = p^2$). Para todo $h \in P$, se tiene que

$$\{g_1h, g_2h, \cdots g_nh\} = \{g_1, g_2, \cdots g_n\}$$

y como Q es abeliano, se tiene que $\overline{y} = y^{g_1}y^{g_2}\cdots y^{g_n}$ verifica que

$$\overline{y}^h = y^{g_1h}y^{g_2h}\cdots y^{g_nh} = \overline{y}$$

y tomando un $h \neq 1$, obtenemos por la hipótesis que

$$\overline{y} = y^{g_1}y^{g_2}\cdots y^{g_n} = 1.$$

Podemos hacer lo mismo con un subgrupo H de P, que tenga p elementos y se tendría que

$$\prod_{g \in H} y^g = 1.$$

Los elementos distintos de la identidad del grupo P son todos de orden p y dos sugrupos de orden p distintos tienen intersección trivial. Como también tenemos que en un grupo de orden p tiene $p-1$ elementos que lo generan, tenemos en P exactamente $\frac{p^2-1}{p-1} = p+1$ subgrupos y cada uno de los p^2-1 elementos distintos de la identidad del grupo P están exactamente en uno de ellos.

Sean $H_1, \cdots H_m$ todos los subgrupos de P de p elementos ($m = p+1$), se tiene

$$1 = \overline{y} = y^{g_1}y^{g_2}\cdots y^{g_n} = y^1 \prod_{1 \neq g \in H_1} y^g \cdots \prod_{1 \neq g \in H_m} y^g.$$

Multiplicamos por y p veces para que en los productos salgan todos los elementos de H_i y obtenemos

$$y^p = \prod_{g\in H_1} y^g \cdots \prod_{g\in H_m} y^g = 1.$$

De donde se deduce que el orden de y es p, en contra de que $y \in Q$ y por tanto tiene orden q. □

Lema 2.56. *Sean p y q primos distintos, P un p-subgrupo de G y Q un q subgrupo de G tal que $P \leq N_G(Q)$.*

Se tiene:

a) $Q = [Q,P]C_Q(P)$.

b) Si además P es elemental abeliano no cíclico, $Q =< C_Q(x) | 1 \neq x \in P >$.

Demostración. a) Suponemos que G es el producto semidirecto $G = [Q]P$ y $Q \trianglelefteq G$. Se tiene que para todo $p \in P$, $q \in Q$, $qpq^{-1}p^{-1} \in Q$ luego $[Q,P] \leq Q$.

También es claro que $P \leq N_G[Q,P]$, sea $y \in P$

$$[q,p]^y = (q^{-1}p^{-1}q)^y p^y = y^{-1}q^{-1}p^{-1}qyp^y = (qy)^{-1}p^{-1}qyp^y = (yq_2)^{-1}p^{-1}yq_2p^y = q_2^{-1}(p^y)^{-1}q_2p^y \in [Q,P]$$

luego si $K = [Q,P]P \leq G$, $P \leq N_G(K)$. Veamos ahora que también Q normaliza a K.

Si $q \in Q$ y $p \in P$, $p^q = q^{-1}pq = q^{-1}pqp^{-1}p \in [Q,P]P = K$, luego $P^Q \leq K$ y comprobamos que $Q \leq N_G(K)$; sea $x \in Q$

$$[q,p]^x = (q^{-1}p^{-1}q)^x p^x = x^{-1}q^{-1}p^{-1}qxp^x = (qx)^{-1}p^{-1}(qx)p^x = q_2^{-1}p^{-1}q_2p^x = q_2^{-1}p^{-1}q_2pp^{-1}p^x \in K.$$

Así $\forall x \in Q$ se tiene $([q,p]p')^x \in K$ luego $K \trianglelefteq G$.

P es un p- subgrupo de Sylow de K y para todo $g \in G$ se tiene que $P^g \leq K$ (por ser $K \trianglelefteq G$) y por ser todos los P-Sylow de K conjugados, existe $k \in K$ tal que $P^g = P^k$, de donde se deduce que $gk^{-1} \in N_G(P)$ y $g \in KN_G(P)$ (Argumento de Frattini (2,51)). Así tenemos que

$$G = KN_G(P) = [Q,P]N_G(P)$$

y por el lema (2,4)

$$Q = Q \cap [Q,P]N_G(P) = [Q,P](N_G(P) \cap Q) = [Q,P]N_Q(P).$$

Por ser $Q \trianglelefteq G$, $[N_Q(P),P] \leq Q \cap P = 1$, luego $N_Q(P) = C_Q(P)$ y $Q = [Q,P]C_Q(P)$.

b) Procedemos por inducción sobre $|P| + |Q|$.

Supongamos primero que existe $1 \neq Q_0 < Q$ y tal que $Q_0 \trianglelefteq G$. Sea $x \in P$ y $R/Q_0 = C_{Q/Q_0}(xQ_0)$. Se tiene que $[R, < x >] \leq Q_0$ y aplicando el apartado a) a los grupos R y $< x >$ (se verifica que $x \in N_G(R)$) se tiene que $R = [R, < x >]C_R(< x >) \leq Q_0C_Q(x)$, de donde deducimos que $R = Q_0C_Q(x)$. Por la hipótesis de inducción $Q/Q_0 =< Q_0C_Q(x)/Q_0 | 1 \neq x \in P >$ y $Q = Q_0 < C_Q(x) | 1 \neq x \in P >$.

También por a hipótesis de inducción, $Q_0 =< C_{Q_0}(x) | 1 \neq x \in P > \leq < C_Q(x) | 1 \neq x \in P >$, luego $Q =< C_Q(x) | 1 \neq x \in P >$.

Ahora podemos ya suponer que Q es normal minimal en G y por tanto Q es elemental abeliano (ver (2,43)) y por lo tanto existe un $x \in P$ tal que $C_Q(x) > 1$.

Veamos que $C_Q(x)$ es normalizado por P. Si $p \in P$ y $q \in C_Q(x)$, como $x^p = x$, se tiene que $[q^p,x] = [q^p,x^p] = [q,x]^p = 1^p = 1$, luego $q^p \in N_G(C_Q(x))$, así que $C_Q(x) \trianglelefteq G$ y por la minimalidad de Q, $Q = C_Q(x)$. □

Definición 2.57. Sea p un número primo, el grupo $GL(n,p)$ es el grupo de matrices nxn de elementos de Z_p. Como el grupo Z_p^n es aditivo, Z_p es también espacio vectorial de dimensión n. Y el grupo de los automorfismos de Z_p^n es $GL(n,p)$.

$$|GL(n,p)| = \prod_{i=0}^{n-1}(p^n - p^i)$$

$SL(n,p)$ el el subgrupo de $GL(n,p)$ cuyas matrices tienen determinante 1.

$$|SL(n,p)| = \prod_{i=0}^{n}(p-(i-1))$$

$SL(n,p) \trianglelefteq GL(n,p)$

Teorema 2.58. ***Teorema de Schur-Zassenhaus***
Sea $N \trianglelefteq G$ tal que $|N| = n$ y $|G/N| = m$ son primos entre sí y N es abeliano, entonces existe un complemento en G de N.

Demostración. Consideramos el homomorfismo $G \to AutN$ dado por la conjugación. Por ser N abeliano, está contenido en el núcleo y se tiene un homomorfismo $G/N \to AutN$ de modo que para cada $gN = x$ el homorfismo $N \to N$ dado por $a \to a^g$ no depende del representante g de $gN = x$. Denotaremos $a^x = a^g$ si $g \in x$.

Sea $\{t_x \in x | x \in G/N\}$ un conjunto de representantes de las distintas clases módulo N (un transversal). Para cada $x, y \in G/N$ se tiene que existe $c(x,y) \in N$ tal que

$$t_x t_y = t_{xy} c(x,y).$$

Se tienen las igualdades

$$(t_x t_y)t_z = t_{xy}c(x,y)t_z = t_{xy}t_z t_z^{-1}c(x,y)t_z = t_{(xy)z}c(xy,z)c(x,y)^{t_z} = t_{(xy)z}c(xy,z)c(x,y)^z$$

$$t_x(t_y t_z) = t_x t_{yz} c(y,z)t_z = t_{x(yz)}c(x,yz)c(y,z).$$

De donde se deduce

$$c(xy,z)c(x,y)^z = c(x,yz)c(y,z).$$

Para cada $y \in G/N$ consideramos el siguiente producto de m elementos de N

$$d(y) = \prod_{x \in G/N} c(x,y).$$

Considerando la igualdad obtenida, haciendo el producto para todos los $x \in G/N$ (y y z fijos) y teniendo en cuenta que el producto en N es conmutativo y que si x recorre todos los elementos de G/N también lo hace xy, se tiene

$$d(z)d(y)^z = d(yz)c(y,z)^m.$$

Como m es primo con el orden de N, se tiene que la aplicación $N \to N$ dada por $e(a) = a^m$ es biyectiva y para cada $y \in N$ existe $e(y) \in N$ tal que $e(y)^m = d(y)^{-1}$.

Sustituyendo en la igualdad, se tiene

$$(e(z)e(y)^z)^{-m} = e(yz)^{-m}c(y,z)^m \Longrightarrow e(yz)^m = (e(z)e(y)^z)^m c(y,z)^m$$

y por tanto

$$e(yz) = e(z)e(y)^z c(y,z).$$

Definimos $s_x = t_x e(x)$ y se tiene

$$s_y s_z = t_y e(y) t_z e(z) = t_y t_z t_z^{-1} e(y) t_z e(z) = t_{yz} c(y,z) e(y)^{t_z} e(z) = t_{yz} c(y,z) e(y)^z e(z) = t_{yz} e(yz) = s_{yz}$$

luego la aplicación $G/N \to G$ dada por $x \to s_x$ es homorfismo, claramente inyectivo por ser $s_x \in x$ y la imagen es un subgrupo H de G que tiene orden $m = |G/N|$. Ademas $H \cap N = s_1 \in N$ solo tiene un elemento luego debe de ser 1 y por el orden $HN = G$. □

Capítulo 3

Teorema $p^a q^b$ de Burnside

Teorema: Burnside [1]

Sea G un grupo de orden $p^a q^b$, con p y q primos. Entonces G es un grupo soluble.

Demostración. La demostración que vamos a realizar está compuesta de diferentes partes a través de las cuales llegaremos a la conclusión del Teorema que estamos estudiando.

Vamos a proceder por reducción a lo absurdo, suponiendo que la hipótesis es falsa intentaremos llegar a una contradicción. Vamos a utilizar un contraejemplo minimal para llegar a esta contradicción.

En todo lo que sigue supongamos que G es un grupo no resoluble cuyo orden es $p^a q^b$ con p y q primos tal que el orden de G es mínimo posible con estas condiciones. Es decir, cualquier H cuyo orden sea producto de potencia de dos primos cumpliendo $|H| < |G|$, será resoluble.

AFIRMACIÓN 1.
G es un grupo no abeliano, simple, con p y q primos distintos y cuyos subgrupos son resolubles.

Demostración. Todo grupo abeliano es resoluble, por lo que G no es abeliano.

Si G no fuera simple, existiría un subgrupo $N \trianglelefteq G$ tal que $N \neq 1$ y $N \neq G$.

Teniendo en cuenta que el orden de N es divisor del orden de G y que este es el grupo de orden mínimo no resoluble, N tiene que ser resoluble. Por el mismo razonamiento $\dfrac{G}{N}$ también tiene que ser resoluble.

Pero por (2,40) G debería ser un grupo resoluble lo que contradice la hipótesis, entonces, G es simple.

Supongamos ahora que p=q entonces tendremos que el orden de G será potencia de un primo y por el lema 2,41 sabemos que $Z(G) \neq \{1\}$ por definición de centro es un subgrupo normal de G. Tomando $Z(G) = N$ (del razonamiento anterior) tendríamos que con estas condiciones G sería resoluble, esto prueba que todo p-grupo es resoluble. Luego p y q son primos distintos.

Por otro lado, el orden de todo subgrupo de G divide al orden de este, en particular es menor y por consiguiente los subgrupos propios de G serán resolubles.

□

Comentario de notación: Deberíamos asumir a partir de ahora que p < q. Para presentar sin sesgos estos resultados que son simétricos en p y q, a lo largo de la demostración {r, s} denotará al par desordenado {p, q}

AFIRMACIÓN 2.
Si G tiene subgrupos A y B tales que $G = AB$ y $A \neq G$, entonces B no normaliza a ningún s-subgrupo no trivial de A.

Demostración. Si $1 \neq H \leq A$, es decir, H es un subgrupo no trivial de A y $B \leq N_G(H)$. Entonces

$$H^{BA} = (BA)^{-1} H (BA) = A^{-1} \underbrace{B^{-1} H B}_{H} A = A^{-1} H A = H^A \tag{3.1}$$

y

$$1 \neq < H^G > = < H^{BA} > \underbrace{=}_{3,1} < H^A > \leq A < G.$$

Por lo tanto, G tendría un subgrupo normal y esto no puede ser porque G es simple. Luego B no normaliza a ningún subgrupo no trivial de A.

□

AFIRMACIÓN 3.
Si $R \in Syl_r(G) \Longrightarrow R$ no normaliza a ningún s-subgrupo de G.

Demostración. Este lema es un caso particular de la Afirmación 2. Bastaría con tomar $R = B$ y A cualquier s-subgrupo de Sylow de G, ya que por el lema 1.4 tenemos que $G = AB$.

□

AFIRMACIÓN 4.
Si $S \in Syl_s(G)$ y $1 \neq Y \trianglelefteq R \in Syl_r(G)$, entonces $G = < S, Y >$.

Demostración. Tomando $R = G$ e $Y = N$ en el lema 2,41, $Y \cap Z(R)$ contiene un elemento $z \neq 1$. Este z estabiliza a todos los elementos de R y teniendo en cuenta que $R \leq G$ se tiene

$$R \leq C_G(z) \leq G.$$

Sea $A = < S, z >$ y $B = C_G(z)$ entonces $G = SR \leq AB$. Siendo que B normaliza al subgrupo no trivial $< z >$ de A, por la Afirmación 2 se tiene que cumplir $G = A$ y por lo tanto $G = < S, Y >$. □

AFIRMACIÓN 5.
Sean M y H subgrupos maximales de G. Asumimos que M tiene r- y s-subgrupos normales no triviales R y S respectivamente tales que $RxS \leq H$. Entonces:

a) $RxS \leq F(H) \leq M$.

b) $M = H$.

Demostración. Siendo $S \trianglelefteq M$ por definición de subgrupo normal y de normalizador se cumplirá $M \leq N_G(S) \leq G$ y por ser G simple y M maximal $M = N_G(S)$. Seguimos el mismo razonamiento para R y tendremos que:

$$N_G(R) = M = N_G(S).$$

Ya que $C_H(R) \leq C_G(R) \leq N_G(R) = M = N_G(S),\ S \trianglelefteq C_H(R)$.

Por otro lado como H es resoluble podemos aplicar el lema $(2{,}54)$ a H y a R para concluir que

$$1 \neq S \leq O_{r'}(C_H(R)) \leq O_{r'}(H) = O_s(H).$$

Con un razonamiento idéntico tendremos que:

$$1 \neq R \leq O_{s'}(C_H(S)) \leq O_{s'}(H) = O_r(H).$$

Hemos obtenido $S \trianglelefteq C_H(R) \leq C_G(R)$, por lo tanto:

$$1 \neq O_s(H) \leq C_G(R) \leq M \quad \text{y} \quad 1 \neq O_r(H) \leq C_G(S) \leq M$$

Unimos todo y

$$RxS \leq O_r(H)xO_s(H) = F(H) \leq M \text{ se cumple a).}$$

Para demostrar b). Podemos revertir los papeles de M y H en el argumento anterior, reemplazando R y S por $O_r(H)$ y $O_s(H)$ respectivamente y concluyendo que el apartado a) se cumple de la misma forma, teniendo como resultado

$$F(H) = O_r(H)xO_s(H) \leq F(M) \leq H.$$

Y aplicando el argumento inicial una vez más con M y H en sus papeles originales pero con $O_r(M)$ y $O_s(M)$ en el lugar de R y S concluimos que $F(M) = O_r(M)xO_s(M) \leq F(H)$. Por lo tanto $F(M) = F(H)$ y en consecuencia tenemos que $M = N_G(F(M)) = N_G(F(H)) = H$. Se cumple b). □

AFIRMACIÓN 6.
Si $M < G$ maximal, entonces $F(M)$ tiene orden potencia de primo.

Demostración. Supongamos que $O_r(M) \neq 1 \neq O_s(M)$ y llegaremos a una contradicción: Sean $R_0 = Z(O_r(M))$ y $S_0 = Z(O_s(M))$, tenemos que R_0 y S_0 son subgrupos normales de M y por el lema 2,41 son no triviales. Tomamos un $x \neq 1$ tal que $x \in F(M) = O_r(M)xO_s(M)$, entonces $R_0xS_0 \leq C_G(x)$ y si aplicamos el apartado b) anterior, con $C_G(x) \leq H$ maximal , tendremos que $C_G(x) \leq M$.

Afirmamos que R_0 es cíclico. Si este no fuera el caso, podríamos encontrar un subgrupo elemental abeliano T de R_0 de orden r^2. Sea $R \in Syl_r(M)$ y normalizador de S_0, la Afirmación 3 implica que $R \notin Syl_r(G)$, por lo que consideremos a U r-grupo de Sylow de G. Notemos que $R = U \cap M$ y por (2,42) $R < N_U(R) \leq N_G(R)$, luego existirá un g tal que pertenezca a U y al $N_G(R)$ pero que no pertenezca a R. Para este elemento también se cumple que $g \in N_G(R) - M$, entonces tendremos

$$T \leq R = R^g \leq M^g \neq M$$

donde T normaliza al subgrupo normal $S = S_0^g$ de M^g y por 2.56

$$S =< C_S(x) | 1 \neq x \in T > \leq < C_G(x) | 1 \neq x \in T > \leq M$$

Entonces M contiene a R_0^g y a S_0^g, $R_0^g x S_0^g \trianglelefteq M^g$, aplicando la Afirmación 5 obtenemos que $M \leq M^g$. Esta contradicción prueba que R_0 es cíclico. De forma similar vemos que S_0 también es cíclico.

Para seguir con la demostración, a partir de aquí vamos a sustituir s y r por p y q debido a que nos interesa cual de estos números es el mayor.

Se sigue que el grupo no identidad $P_0 = Z(O_p(M))$ también es cíclico. Sea $|P_0| = p^c$ y sea $Q \in Syl_q(M)$. Puesto que el orden del q-grupo de automorfismo inducidos por Q en P_0, $|Aut(P_0)|$, es igual a $p^{c-1}(p-1)$ indica que Q centraliza a P_0 porque como dice la hipótesis p<q. Así, $P_0xQ_0 \leq N_G(Q)$, donde $1 \neq Q_0 = Z(O_p(M))$ y por la Afirmación 5 $N_G(Q) \leq M$. Pero entonces $Q \in Syl_q(G)$ lo cual es imposible porque Q normaliza a P_0 (Afirmación 3)

Y con esta última contradicción concluimos que ó $O_p(M) = 1$ ó $O_q(M) = 1$ □

Definición 3.1. Sea t primo y E grupo finito. Un t-subgrupo $U \subseteq E$ se denomina localmente central si $U \leq Z(T)$ para algún $T \in Syl_t(E)$

AFIRMACIÓN 7.
Si un subgrupo maximal M de G contienen a un r-subgrupo localmente central distinto a la identidad Y, entonces $F(M)$ es un r-grupo.

Demostración. Supongamos por el contrario que $F(M)$ es un s-grupo, lo que por la Afirmación 6 es la única alternativa. Elegimos un s-grupo de Sylow que contenga a $F(M)$ y denotamos su centro con Z.

Como $C_G(F(M)) \leq N_G(F(M)) = M$ y por 2,53, es claro que

$$Z \leq C_G(F(M)) \leq C_M(F(M)) \leq F(M)$$

Sea

$$L =< Z^y | y \in Y > \Longrightarrow L \leq F(M).$$

Debido a que Y normaliza a F(M) y Z es normal en M y además L es un subgrupo normalizado por Y

Denotamos $\mathscr{M}$ al conjunto de todos los s-subgrupos de G tales que :

1. Son normalizados por Y.
2. Son generados por los conjugados de G en Z.

Entonces $1 \neq L \in \mathscr{M}$

Sea K un elemento maximal de $\mathscr{M}$ que contiene a L y sea S un s-Sylow de G que contiene a K. Como Y es localmente central, podemos aplicar Afirmación 4 y tendremos que $G =< S, Y >$, y por definición de $\mathscr{M}$ Y normaliza a K. Por lo que S no normalizará a K y por (2,42) podremos encontrar un elemento

$$x \in N_S(N_S(K)) - N_S(K) \Longrightarrow K \neq K^x \leq N_S(K).$$

Como K^x está generado por ciertos conjugados de Z, uno de ellos, llamado Z^g, no está contenido en K y como Y es localmente central, se cumple

$$G = C_G(Z)C_G(Y).$$

Escribimos $g = uv$ con $u \in C_G(Z), \quad v \in C_G(Y)$ y concluimos que

$$Z^g = Z^{uv} = (u^{-1}Zu)^v = Z^v \nleq K.$$

Sea

$$L^* =< Z^{vy} | y \in Y >=< Z^y | y \in Y >^v = L^v$$

En consecuencia L^* es un s-grupo normalizado por Y y como $Y, Z^v \leq N_G(K)$ se sigue que L^*normaliza a K.

Por lo tanto, KL^* es un s-grupo normalizado por Y y generado por conjugados de Z. Pero $Z^v \nleq K$ y KL^* será un elemento de $\mathscr{M}$ que contiene estrictamente a k.

Esto contradice la elección de K como elemento maximal y se tendrá que $F(M)$ es como Y, un r-grupo. □

AFIRMACIÓN 8.
Un r-subgrupo $Y \neq 1$ de G, que es localmente central, no normaliza a ningún s-subgrupo no trivial de G.

Demostración. Si S es un s-subgrupo de G normalizado por Y, un subgrupo maximal M de G conteniendo a $N_G(S)$ contiene a Y, así como el centro, Z, de un s-Sylow que contiene a S de G.

Ahora Z es, indudablemente, localizador central contenido en M y por Afirmación 7 el subgrupo Fitting de M es al mismo tiempo r-grupo y s-grupo y por consiguiente es trivial. Esto contradice la resolubilidad de M e Y no normaliza a S. □

AFIRMACIÓN 9.
G tiene orden impar.

Demostración. Si G es de orden par, indudablemente uno de los dos primos que dividen su orden es el 2. El centro de un 2-Sylow de G contiene un elemento x de orden 2, es decir, $x = x^{-1}$. Dicho elemento normaliza a algún subgrupo de orden impar no trivial y esto claramente contradice la Afirmación 8 dado que el centro del 2-Sylow localmente central.

Luego el orden de G es impar. □

AFIRMACIÓN 10.
Sea R_0 un r-subgrupo de no trivial de G y sea

$$C_G(R_0) \leq L \leq G$$

Además, sea $R_0 \leq R_1 \leq R_2$ con $R_1 \in Syl_r(L)$ y $R_2 \in Syl_r(G)$

Entonces tenemos:

a) $F(L) = O_r(L)$.

b) $\Omega(Z(R_2)) \leq \Omega(Z(O_r(L)))$.

c) $C_G(\Omega(Z(O_r(L))))$. es un r-grupo.

Demostración.

$$1 \neq Z(R_2) \leq C_G(R_0) \leq L$$

y como $Z(R_2)$ es un r-grupo localmente central de G por Afirmación 8 no normaliza a ningún s-subgrupo no trivial de G y tendremos $O_s(L) = 1$, por lo tanto $F(L) = O_r(L)$.

Como $O_r(L) \leq R_1 \leq R_2$, por la estructura de G y la proposición 2,53 (L es resoluble)

$$Z(R_2) \leq C_L(F(L)) \leq F(L)$$

luego

$$Z(R_2) \leq Z(O_r(L))$$

y se cumple b).

Finalmente sea $S \in Sly_s(C_G(\Omega(Z(O_r(L)))))$. Por b) se deduce que s y $\Omega(Z(R_2))$ conmutan entre sí, como $\Omega(Z(R_2))$ es un r-grupo localmente central tenemos que se tiene que cumplir $S = 1$ y por la Afirmación 8 se cumple el apartado c).

□

AFIRMACIÓN 11.
Si P_0 es un p-subgrupo de G no trivial, entonces $N_G(P_0)$ tiene un q-subgrupo de Sylow cíclico.

(recordamos que p<q)

Supongamos por el contrario que G tienen un p-subgrupo $P_0 \neq 1$ cuyo normalizador tiene un q-subgrupo de Sylow no cíclico, y sea $V = \Omega(Z(P_0))$.

Como $N_G(V) \supseteq N_G(P_0)$, también contiene a un subgrupo elemental abeliano de orden q^2. Así el conjunto $\mathscr{N}$ de los pares ordenados (A,V) satisface:

1. A es elemental abeliano de orden q^2
2. V es un maximal es un p-subgrupo elemental abeliano invariante con A de G y $V \neq 1$, no vacío. Y de esto derivaremos a una contradicción.

Sea (A,V) un par en $\mathscr{N}$ con $|C_V(A)|$ lo más grande posible.

Primero afirmamos que

$$V > C_V(A) \text{ (veamoslo)} \tag{3.2}$$

Sea $Y = \Omega(Z(O_P(N_G(V))))$, y aplicando Afirmación 10 con $V, N_G(V)$ y p en los papeles de R_0, L y r respectivamente concluimos que $C_G(Y)$ es un p-grupo. Sin embargo, Y es un p-subgrupo elemental abeliano invariante con A del centro de $O_P(N_G(V))$, que obviamente contiene a V, y en consecuencia VY es un elemental abeliano invariante con A. Por lo tanto $Y \leq V$, debido a la elección de V en la definición de $\mathscr{N}$ y se sigue que $C_G(V) \subseteq C_G(Y)$. Así, $C_G(V)$ es un p-grupo y 3,2 está justificada.

Por (2,56) tenemos que $V =< C_V(x) | 1 \neq x \in A >$, así existirá un elemento $x \in A - \{1\}$ tal que el subgrupo $U = C_V(x)$ contien adecuadamente a $C_V(A)$. Como A centraliza a x, U es invariante con A y obviamente no está centralizado por este. Luego por $(ref\,1{,}27)$ el subgrupo induce en $U/C_V(A)$ a un p-grupo no trivial de automorfismos, y como p<q y $|Aut(Z_p)| = p-1$, concluimos que

$$|U/C_G(A)| \geq p^2 \tag{3.3}$$

Demostración. Sea $Z_1 = \Omega(Z(O_q(C_G(x))))$ y tenemos en cuenta que $1 \neq x \in Z_1$. Aplicando Afirmación $(10)(c)$, esta vez con $< x >, C_G(x)$ y q en lugar de R_0, L y r, vemos que $C_G(Z_1)$ es un q-grupo. Como $1 \neq U \leq C_G(x)$, se sigue que Z_1 es normalizado pero no centralizado por U. Por lo tanto el grupo de automorfismos inducidos por U en la sección $Z_1/ < x >$ es no trivial. Por 2.56 hay un subgrupo W de indice p en U que centraliza a un subgrupo no tribial $Z_2/ < x >$ de $Z_1/ < x >$, y W centraliza a Z_2.

Como Z_1 es abeliano elemental, se sigue que Z_2 contiene un subgrupo abeliano elemental, A_1, de orden q^2, y porque A_1 centraliza a W podemos encontrar un p-subgrupo abeliano elemental, invariante con A_1 y maximal contenido en W, que llamaremos V_1. Entonces, evidentemente $(A_1, V_1) \in \mathscr{N}$ y $W \leq C_V(A_1)$. Pero por 3,3 tenemos que

$$|W| = |U|/p > |C_V(A_1)|$$

que contradice la elección del par (A,V). Por lo tanto se cumple 2.12 □

AFIRMACIÓN 12.
Sea M un subgrupo maximal de G, y asumimos que $F(M)$ es un r-grupo. Entonces $M/F(M)$ tiene un r-subgrupo de Sylow cíclico.

Demostración. Sea $R = F(M)$ y sea $SR/R = F(M/R) = O_s(M/R)$ con $S \in Syl_s(SR)$. Aplicamos el argumento de Frattini (2,51) siendo $SR \trianglelefteq M$ y S un s-Sylow de RS, entonces $M = RSN_M(S) = RN_M(S)$.

Si $S = 1$, entonces $M = F(M)$ y el lema sería cierto.

Si $S \neq 1$, hay dos posibilidades:

- Si $s = p$ y por consiguiente $r = q$, aplicando la Afirmación (11) el grupo $N_G(S)$ tiene un r-subgrupo de Sylow cíclico; así $M/F(M) = RN_M(S)/R \simeq N_M(S)/N_R(S)$ también tendrá un r-subgrupo de Sylow cíclico.

- Por otro lado si $s = q$ y $r = p$, como $M = N_G(F(M)) = N_G(R)$ y por la Afirmación 11 M tiene un s-Sylow cíclico. Entonces S estará contenido en este Sylow y como los subgrupos de uno cíclico también son cíclicos, S será cíclico.

  Ahora consideramos el grupo resoluble $M^* = M/F(M)$. Su subgrupo de Fitting es isomorfo a S

  $$F(M^*) = F(\frac{M}{R}) = \frac{SR}{R} \simeq \frac{S}{S \cap R} = S$$

  y por (2,53) se auto centraliza, $C_G(S) \simeq C_G(F(M^*)) \leq F(M^*) \simeq S$. Por lo tanto $M^*/F(M^*)$ es isomorfo con un subgrupo de Aut(S), que es cíclico por ser automorfismo de un cíclico cuyo orden es potencia de un primo. Luego un r-subgrupo de Sylow de M^*, que en este caso es un p-subgrupo de Sylow es también cíclico y con esto queda demostrado el lema.

□

Definición 3.2. Sea R un r-grupo y definimos el subgrupo $J_0(R)$ como el subgrupo de R generado por todos sus subgrupos elementales abelianos de orden máximo.

Claramente $J_0(R)$ es un subgrupo característico de R, y si $J_0(R) \leq U \leq R$, entonces $J_0(R) = J_0(U)$.

AFIRMACIÓN 13.
Sea M subgrupo maximal de G, y asumimos que F(M) es un r-grupo. Si $R \in Syl_r(M)$ entonces $M = N_G(J_0(R))$ y $R \in Syl_r(G)$

Demostración. Sea $K = F(M)$. Vamos a suponer que $J_0(R) \nleq K$ y llegaremos a una contradicción. Entonces entre los subgrupos elementales abelianos de R de orden máximo existirá al menos uno que no esté contenido en K, lo llamaremos A. Teniendo en cuenta que un grupo elemental abeliano de orden máximo es un grupo de Sylow, por la Afirmación (12) tomando $A = S$ y $K = R$ el cociente AK/K es cíclico y por lo tanto

$$|A : A \cap K| = \frac{|A|}{|A \cap K|} = r.$$

Sea $V = \Omega(Z(K))$, y observamos que $(A \cap K)V$ es un subgrupo elemental abeliano de R. Luego:

$$|A| \geq |(A \cap K)V| = \frac{|A \cap K||V|}{|A \cap V|} = \frac{|A||V|}{r|A \cap V|}.$$

Despejamos r y se tiene:

$$r \geq |V : A \cap V| \tag{3.4}$$

Como $1 \neq V$ char $K \trianglelefteq M$ entonces $M \subseteq N_G(V)$ y como $M < \cdot G$, tendremos el otro contenido y por lo tanto la igualdad $M = N_G(V)$. Se sigue que $C_G(V) \leq M$ y aplicamos (Afirmación 10)(c) tomando V por R_0 y M por L, con lo que concluiremos que $C_G(V)$ es un r-grupo; y además es un r-subgrupo normal de M, que por lo tanto coincide con K y entonces $C_G(V) = C_M(V) = K$.

Este resultado, siendo $H = M/K = M/C_M(V)$, nos dice que M actúa por conjugación sobre V e induce un grupo de automorfismos isomorfo con H, como $|V| \leq r^2$ este grupo será $GL(2,r)$. Ahora $SL(2,r)$ es normal en $GL(2,r)$ y tiene índice $(r-1)$ por 2.57, luego todo r-elemento de $GL(2,r)$ se encuentra en $SL(2,r)$. Por lo tanto R es maximal en M, por lo que M y H estarán generados por r-elementos y en consecuencia H es isomorfo a $SL(2,r)$. Sabemos que $|SL(2,r)| = (r-1)r(r+1)$ y además como $O_r(M) = F(M) = K$, tendremos que $O_r(H) = 1$. Sea S s-subgrupo elemental abeliano de H, entonces $|S| = s^m$ con $s^m \equiv 1 \bmod p$. Por lo que tenemos que s divide a $(r-1)$ y a $(r+1)$, por hipótesis r es impar por lo tanto $(r-1)$ y $(r+1)$ son pares y se cumplirá que $s = 2$. Lo que contradice a que G tiene orden impar, luego $J_0(R) \leq K$. Como $J_0(R) \leq K$ que es subgrupo característico de $K \triangleleft M$ y se sigue que $M = N_G(J_0(R))$.

Si $R < R^* \in Syl_r(G)$, tendremos que $J_0(R) char R < N_{R^*}(R)$; pero este no puede ser el caso porque $N_{R^*}(R) \leq N_G(J_0(R)) = M$ y $R \in Syl_r(M)$. Por lo tanto $R \in Syl_r(G)$. □

AFIRMACIÓN 14.
Sea M un subgrupo maximal de G, y asumimos que $F(M)$ es un r-grupo. Si $g \in G - M$, entonces $M \cap M^g$ es un s-grupo.

Demostración. Supongamos que esto no es así, es decir que $M \cap M^g$ no es un s-grupo. Elegimos un $g \in G - M$ y así un r-subgrupo de Sylow R de $M \cap M^g$ tiene el mayor orden posible.

Si $R \in Syl_r(M)$ entonces $R \in Syl_r(M^g)$ y aplicando Afirmación 13 tanto a M como a M^g se tiene que $M = N_G(J_0(R)) = M^g$, es una contradicción ya que $M \neq M^g$ (visto en las apartados anteriores).

Si $1 < R < R_1$ para algún $R_1 \in Syl_r(M)$. Sea H un subgrupo maximal de G conteniendo a $N_G(R)$, aplicando Afirmación $10(a)$ el grupo $F(H)$ es un r-grupo y así se sigue por Afirmación 13 que $H = N_G(J_0(R_2))$ para algún $R_2 \in Syl_r(G)$. También por la Afirmación 13 $R_1 \in Syl_r(G)$ y se sigue de los teoremas de Sylow que R_1 y R_2 son conjugados en G, luego $J_0(R_2)$ y $J_0(R_1)$ también lo serán porque $J_0(X)$ es un subgrupo característico de X. En consecuencia H es conjugado de $N_G(J_0(R_1)) = M$. Como $R < N_{R_1}(R) \leq H \cap M$, la elección de R y M^g fuerza $H = M$. Aplicando un argumento idéntico sobre R vemos como un subgrupo de M^g produce que $H = M^g$, y otra vez tenemos la contradicción de que $M = M^g$.

Por lo tanto $M \cap M^g$ debe ser un s-grupo. □

La conclusión de la demostración del teorema de Burnside.

Analicemos las consecuencias de las afirmaciones que hemos probado hasta el momento.

Tomamos r y s como los dos números primos que dividen al orden de G. De esta manera no sabemos cual de los dos es el mayor. Pero los identificamos dela siguiente manera: Sea R el r-subgrupo de Sylow de G y S el s-subgrupo de Sylow de G tales que $|R| > |S|$

Por otra parte, sea M el subgrupo maximal de G conteniendo a $C_G(Z(R))$. Por Afirmación 10(a) sabemos que $F(M)$ es un r-grupo.

Si $g \in G - M$, por Afirmación 14 la intersección de M y M^g es un s-grupo, luego $R \cap R^g = 1$. Por lo tanto RR^g es un subconjunto de G que contiene $|RR^g| = |R||R^g| = |R|^2$ elementos. Sin embargo, $|R|^2 > |R||S| = |G|$, contradicción.

Y con esta última contradicción termina la demostración ya que no puede existir un grupo con las condiciones dadas. Por lo tanto tenemos que G es resoluble. □

Capítulo 4

Subgrupos de Hall

Definición 4.1. (a) Sea π un conjunto de primos, un subgrupo H de un grupo G es llamado π-subgrupo de Hall si $|H|$ es un π-número y $|G:H|$ es un π'-número. El conjunto de los π-subgrupos de Hall de G será denotado por $Hall_\pi(G)$

(b) Un subgrupo H de G es llamado subgrupo de Hall si es un π-subgrupo de Hall para algún π (conjunto de primos). Evidentemente H es un subgrupo de Hall de G si y solo si $(|G:H|,|H|)=1$.

Observaciones: Recordamos que $\sigma(G)$ es el conjunto de todos los primos que dividen al orden de G.

1. Sea H π-subgrupo de Hall y X π-subgrupo tal que $H \leq X$, entonces $H = X$. Y se que H es un π-subgrupo maximal.
2. Sea p primo, entonces $Hall_p(G) = Syl_p(G)$.
3. Sea p primo, $P \in Syl_p(G)$ y $H \in Hall_{p'}(G)$, entonces $G = HP$ y $H \cap P = 1$. Por esta razón los p'-subgrupos de Hall son a veces llamados p-complementos de Sylows.

Teorema 4.2. *Un grupo finito G es resoluble si y solo si posee π-subgrupos de Hall para todo conjunto de primos π.*

Demostración. La demostración de este teorema, realizada en ambos sentidos por separado, se encuentra reflejada en 4.3 para la implicación de izquierda a derecha, y en 4.6 para la implicación inversa. Para esta última será necesario 4.4 y 4.5. □

Teorema 4.3. *Sea G un grupo resoluble y π un conjunto de primos. Entonces existe al menos un π-subgrupo de Hall.*

Demostración. Probaremos esta conclusión por inducción sobre $|G|$. Si $G = 1$ el resultado es trivialmente cierto, por lo tanto, supongamos que $G \neq 1$ y sea N un subgrupo normal minimal de G, que por (2,43) este subgrupo N es un p-grupo para algún p primo.

Por inducción G/N tiene un π-subgrupo de Hall H/N.

Si $p \in \pi$ se tendrá que H es un π-grupo y como

$$|\frac{G}{N} : \frac{H}{N}| = \frac{|\frac{G}{N}|}{|\frac{H}{N}|} = \frac{|G:N|}{|H:N|} = |G:H| \text{ es } \pi' - \text{número}$$

por lo tanto H es un π-grupo de Hall de G.

Si $p \notin \pi$ por el teorema del complemento de Zassenhaus (2,58) existe un complemento de N en H, es decir, existe $U \leq H$ tal que $N \cap U = 1$ y $NU = H$. Entonces se tendrá que

$$\frac{H}{N} = \frac{NU}{N} \simeq \frac{U}{N \cap U} = U$$

y $|U| = \frac{|H|}{|N|}$ es π-número. Por otro lado $|G:U| = |G:H||H:U| = |G:H|\frac{|H|}{|U|} = |G:H||N|$ es un π'-número, luego se sigue que U es un π-subgrupo de Hall de G

Y tenemos probada la existencia. □

Teorema 4.4. *Si un grupo G tiene tres subgrupos resolubles H_1, H_2 y H_3 cuyos índices son coprimos dos a dos, entonces G también es resoluble.*

Demostración. Por ser los índices coprimos, aplicando el lema 2,11 y obtenemos $G = H_1H_2 = H_1H_3 = H_2H_3$, podemos suponer que $H_1 \neq 1$.

Sea N un subgrupo normal minimal de H_1, hemos visto anteriormente que este tipo de subgrupos son p-grupos. No podemos saber si p es divisor de $|G:H_1|$ pero como también $|G:H_2|$ es coprimo con $|G:H_3|$ al menos uno de estos dos índices no será divisible por p, sin perdida de generalidad tomamos que p no divide a $|G:H_2|$.

Sea $D = H_1 \cap H_2$, ya que $N \trianglelefteq H_1$ el producto $ND \leq H_1$ y $|ND:D| = |N:N\cap D| = p^n$ para algún n, este valor divide a $|H_1:D| = |H_1H_2:H_2| = |G:H_2|$ pero p no divide a $|G:H_2|$. Por lo tanto, $|N:N\cap D| = 1$ y $N \leq D$.

Sea $K = N^G \trianglelefteq G$, entonces $K =< N^{h_1h_2} | h_i \in H_i >=< N^{h_2} | h_2 \in H_2 > \leq H_2$, en consecuencia, como K es subgrupo de un grupo resoluble, es resoluble. POr otro lado, los subgrupos $\{H_iK/K | i = 1,2,3\}$ son resolubles y tienen parejas de índices coprimos en G/K. Como $K \neq 1$, podemos suponer por inducción sobre el orden grupal que G/K es resoluble. Luego aplicando(2,40), siendo $K \trianglelefteq G$ y resoluble y G/K resoluble, G es resoluble. □

Teorema 4.5. *Sea G un grupo tal que $|G| = \prod_{j=1}^{r} p_i^{a_i}$, donde $p_1, \cdots, p_r$ son primos distintos. Si G tiene p-complementos de Sylows para todo p primo divisor de su orden, es decir, $\forall p_i$ divisor de $|G|$ existe un p_i'-subgrupo de Hall de G, entonces G es resoluble.*

Demostración. Lo probamos por inducción sobre $r = |\sigma(G)|$.

Si $r \leq 2$, G es soluble por el teorema p^aq^b de Burnside, estudiado en el Capítulo 2.

Si $r \geq 3$, asumimos que G posee subgrupos $S_1, \cdots, S_r$ tales que $|G:S_i| = p_i^{a_i}$ con $i = 1, \cdots, r$, luego todos estos índices son coprimos dos a dos. Tomamos S_i cualquiera de los r subgrupos de G citados. Sea $1 \leq i \neq j \leq r$ y sea $T_{ij} = S_i \cap S_j$ como $(|G:S_i|, |G:S_j| = 1 \Longrightarrow G = S_iS_j)$ y por lo tanto, $p_j^{a_j} = |G:S_j| = |S_i:T_{ij}|$. Así T_{ij} es un p_j-complemento de Sylow de S_i, siendo $P_j \in Syl_{pj}(S_i)$, $\quad S_i = P_jT_{ij}$, esto se cumple $\forall j \neq i$. Por consiguiente S_i cumple la hipótesis del teorema y hemos visto que $|\sigma(S_i)| = r-1$, todos los que dividen al orden de G menos p_i, por inducción sobre r tendremos que S_i será resoluble $\forall 1 \leq i \leq r$.

Ahora tomamos tres cualesquiera de estos sungrupos de G, por ejemplo, S_1, S_2, S_3 que como hemos visto son todos resolubles y por hipótesis sus índices, $|G:S_1|, |G:S_2|, |G:S_3|$ son coprimos dos a dos, por el teorema (4.4) obtenemos que G es resoluble. □

Claramente este Teorema es una generalización del Teorema de Burnside, estudiado con detalle en el capitulo dos.

Corolario 4.6. *Si un grupo finito G posee π-subgrupos de Hall para todo conjunto de primos π, entonces es resoluble.*

Demostración. Es un resultado directo del teorema anterior. Si G posee π-subgrupos de Hall para todo conjunto de primos π poseerá p-complementos de Sylow para todo p primo divisor del orden de G y por lo tanto G será resoluble. □

De esta manera concluimos el trabajo, habiendo llegado en este último capítulo a la caracterización de un grupo finito resoluble mediante sus subgrupos de Hall, que era el objetivo de este trabajo.

Bibliografía

[1] KLAUS DOERK Y TREVOR HAWKES, *Finite Soluble Groups*, Walter de Gruyter, Berlin, New York, 1992, 1-83,205-219.

[2] ANTONIO MACHÌ, *An Introduction to Ideas andMethods of the Theory of Groups*, Springer, 2012, 1-249.

[3] PAZ JIMÉNEZ, *Teoría de Galois*, Asignatura teoría de Galois, grado en Matemáticas, Universidad de Zaragoza.

[4] ELENA AUSEJO, *Historia de las Matemáticas*, Universidad de Zaragoza

[5] ENRIQUE R. AZNAR, Dpto. Álgebra, Universidad de Granada `https://www.ugr.es/~eaznar/index.html`

[6] DEREK J.S. ROBINSON, *A Course in the Theory of Groups*, Springer,1995, 253-255, 298-303.

Listado de Definiciones y Notaciones.